Version Number: 01-2019

U.S. Department of Commerce
National Institute of Standards and Technology
(NIST)

Privacy Impact Assessment
for the
183-01 Applications System Division (ASD) - Moderate Applications

Reviewed by: Susannah Schiller, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.10.15 15:19:07 -04'00' 09/30/2020

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Institute of Standards and Technology (NIST)

Unique Project Identifier: 183-01

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
(b) System location
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
(d) The way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

183-01, Application Systems Division (ASD) Moderate Applications Systems, is made up of several enterprise-wide infrastructure subsystems. Following are 183-01 subsystems that may involve PII/BII related data:

- **The Central People Repository (CPR) subsystem is a collection of central database tables which contain information about NIST staff.**
- **The Web Content Management (WCM) subsystem provides a common management tool for NIST operating units (OUs) to create, approve and publish public and internal web pages. WCM includes both implementations that support NIST's public website and NIST's Intranet. The public web pages also host an Organization of Scientific Area Committees (OSAC) Membership Application which allows users to apply for OSAC membership.**
- **The Web Application Server subsystem is an application infrastructure for developing, integrating, securing, and managing distributed applications.**
- **The Reporting Tools subsystem provides reporting capabilities for various applications used throughout NIST.**
- **The Attachment Application subsystem provides an application infrastructure for storing attachments that relates to various NIST's ServiceNow custom applications in a secure repository.**

Of note is that Web Application Server, Reporting Tools and Attachment Application do not process PII/BII data directly, although they may transmit such data from one of the NIST systems that they support.

a. Whether it is a general support system, major application, or other type of system
183-01 is a general support system.

b. System location
The components, except for WCM, are located at the NIST Gaithersburg, Maryland facility within the continental United States. The WCM sites are located in the Acquia Cloud environment which is itself hosted on the Amazon Web Services (AWS) platform.

c. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

- **CPR interconnects with many additional NIST systems. These other interconnected systems, not 183-01, are responsible for the security of this data as it enters their accreditation boundaries respectively.**
- **WCM subsystem has separate internal and external implementations –**

For WCM Intranet Implementation, interconnection in place is:

- **183-01 CPR - syncs data from CPR subsystem through a cron job to provide data for internal phone directory search—it has a CPR database view for purposes of retrieving the needed CPR data for phone directory search functionality.**

For WCM External Implementation, the following key interconnections are in place:

- **600-01 NIKE - obtain copies of approved NIST publications for purposes of allowing users to access those publications through the 'Publications Search' component of the public website.**
- **183-01 CPR - obtain directory data for NIST employees and associates for purposes of displaying that data through the 'People Search' component of the public website.**
- **107-02 Kaltura - storing videos that are accessible through the public website.**

Web Application Server, Reporting Tools, and the Attachment Application interconnect with several other NIST systems. These other interconnected systems, not 183-01, are responsible for the security of this data as it enters their accreditation boundaries respectively.

Notes: These interconnections do not involve direct access to any NIST internal systems and leverage pre-existing capabilities for retrieving data for purposes of displaying that data through the public website.

d. The way the system operates to achieve the purpose(s) identified in Section 4

- **CPR is a collection of central database tables which contain information about NIST staff (i.e., Federal employees and Associates). The CPR receives data from two human resources applications, the Human Resources Arrival and Departure System (HRADS) and NIST Associates Information System (NAIS-Web). Data such as staff arrival and departure dates, general locator, and identifier information of NIST staff (i.e., employee and associate) are recorded in CPR. These data are used to populate enterprise services and applications such as Active Directory, LDAP, and processing of NIST reorganizations. It also assists in the monitoring and closing of information technology accounts.**

In contrast to other 183-01 components, 183-01 actually owns CPR data.

- **WCM component provides NIST operating units (OUs) with a standardized web content management toolset for the creation, approval, and publication of NIST websites.**

Specific to WCM public facing implementation, there is a public facing Organization of Scientific Area Committees (OSAC) Membership Application. This OSAC application allows members of the public to submit required data to apply for membership. The collected data are accessible only by internal NIST users through the internal WCM component.

e. How information in the system is retrieved by the user

- **CPR system serves to provide data feed to other NIST enterprise services and applications as mentioned in previous paragraphs. CPR data cannot be retrieved directly by typical NIST users. The system includes a Central People Application (CPA), which allows management of CPR data elements. CPA access is provided to a limited group of users with specific roles and privileges defined.**
- **For WCM, Phone directory search data is accessed via forms-based directory search capabilities on NIST's public website and Intranet by end users of those sites. Data is submitted to the OSAC Membership Application via a form on NIST's public website and is accessible to a small number of authorized NIST staff on the OSAC selection committee (submitted data is not accessible publicly in any way).**

f. How information is transmitted to and from the system

TLS is used to protect data in transmission to and from the components.

g. Any information sharing conducted by the system

The system shares information with other internal NIST business units, and other DOC units serviced by NIST.

h. The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The National Institute of Standards and Technology Act, as amended, 15 U.S.C. 271 et seq. (which includes Title 15 U.S.C. 272) and section 12 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended, 15 U.S.C. 3710a.
Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

5 U.S.C. App.—Inspector General Act of 1978, § 2; 5 U.S.C. App.—Reorganization Plan of 1970, § 2; 13 U.S.C. § 2; 13 U.S.C. § 131; 15 U.S.C. § 272; 15 U.S.C. § 1151; 15 U.S.C. § 1501; 15 U.S.C. § 1512; 15 U.S.C. § 1516; 15 U.S.C. § 3704b; 16 U.S.C. § 1431; 35 U.S.C. § 2; 42 U.S.C. § 3121 et seq.; 47 U.S.C. § 902; 50 U.S.C. App. § 2401 et seq.; E.O. 11625; 77 FR 49699 (Aug. 16, 1012).

i. *The Federal Information Processing Standard (FIPS) 199 security impact category for the system is* **Moderate.**

Section 1: Status of the Information System

1.1 The status of this information system:

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015)

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks:

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated.

Identifying Numbers (IN)
Employer ID
Employee ID
Other identifying numbers:
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

General Personal Data (GPD)
Name
Home Address
Telephone Number
Email Address
Education

Other general personal data
Other general personal data:

Work-Related Data (WRD)
Occupation
Job Title
Work Address
Work Telephone Number
Work Email Address
Work History
Other work-related data:
Service computation date and separation date

Distinguishing Features/Biometrics (DFB)
Other distinguishing features/biometrics:

System Administration/Audit Data (SAAD)
User ID
IP Address
Date/Time of Access
Queries Run
Other system administration/audit data:

Other Information
N/A

2.2 Indicate sources of the PII/BII in the system.

Directly from Individual about Whom the Information Pertains
Hard Copy - Mail/Fax
Online
Other:

Government Sources
Within the Bureau
Other Federal Agencies
Other:

Non-government Sources
Other:

2.3 Describe how the accuracy of the information in the system is ensured.

For CPR, internal processes are in place to permit users (e.g., federal staff and associates) to review their directory information through the Outlook address and NIST phone book on the WCM iNet web page. **The Employee data is updated through the HR managed application HRADS and HRDW while NIST associates' data is updated through the NAIS application. The CPR database has daily scheduled jobs which send emails to the CPR admin for any discrepancy in the data which is corrected by the OU administrative staffs.**

2.4 Is the information covered by the Paperwork Reduction Act?

Yes, the information is covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:
1. OSAC form OMB control number: 0693-0070.

2.5 Is there any technology used that contain PII/BII in ways that have not been previously deployed?

No

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)
Other:

Section 3: System Supported Activities

3.1 Are there any IT system supported activities which raise privacy risks/concerns?

No

The IT system supported activities which raise privacy risks/concerns.

Activities
Other:

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.

Purpose
For administrative matters **To improve Federal services online** **To promote information sharing initiatives**
Other:

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The CPR increases the use of Federal services online by serving as an authoritative enterprise source for applications such as Active Directory, LDAP, and processing of NIST reorganizations. It also assists in the monitoring and closing of information technology accounts. Information within this component supports NIST staff (i.e., employees and associates). **The Web Content Management (WCM) intranet component allow staff directory data from CPR to be searched. The WCM component permits members of the public to submit, through the external website, an OSAC Membership Application. This supports improving Federal services online.**

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Retention schedules are now more firmly implemented. Training occurs as a common control organizationally. An insider threat is a possibility albeit remote. Sensitive PII (SPII) is minimally used (e.g., social security numbers and date of birth have been eliminated since FY17).

Section 6: Information Sharing and Access

6.1 Will the PII/BII in the system be shared?

Yes, the PII/BII in the system will be shared

The recipients the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

Bulk Transfer - DOC bureaus **Case-by-Case - Within the bureau**
Other:

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.
The name of the IT system and description of the technical controls which prevent PII/BII leakage:
The CPR shares information with the following NIST information systems (you may reference the below PIAs which address additional technical controls): **1. 100-03, NIST Associate Information Web System (NAIS)** **2. 172-01, Human Resources System**

3. 137-01, Emergency Services Office (ESO)

6.3 Identify the class of users who will have access to the IT system and the PII/BII.

Class of Users
Government Employees
Other:

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system.

Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9. **Yes, notice is provided by a Privacy Act statement and/or privacy policy.** **No, notice is not provided.**
The Privacy Act statement and/or privacy policy can be found at:
https://www.nist.gov/privacy-policy. **The WCM component (e.g., Application) can be found at https://www.nist.gov/osac-application-form.**
The reason why notice is/is not provided:
No: For CPR data is inherited by other systems which present the requisite notice.

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

Yes, individuals have an opportunity to decline to provide PII/BII. **No, individuals do not have an opportunity to decline to provide PII/BII.**
The reason why individuals can/cannot decline to provide PII/BII:
Yes: The WCM component (e.g., Application) identifies a NIST point of contact if an individual does not wish to accept the risk of electronically submitting information. **No: For CPR, information is inherited by other systems which present opportunity to decline.**

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

Yes, individuals have an opportunity to consent to particular uses of their PII/BII. **No, individuals do not have an opportunity to consent to particular uses of their PII/BII.**
The reason why individuals can/cannot consent to particular uses of their PII/BII:
Yes: The WCM component (e.g., Application) identifies how the information submitted will be used. There are no other uses. **No: For CPR, data is inherited by other systems which address consent of particular uses.**

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

Yes, individuals have an opportunity to review/update PII/BII pertaining to them.
The reason why individuals can/cannot review/update PII/BII:
For WCM, individuals have opportunity to review/update their information by contacting the identified NIST point of contact. **For CPR, internal processes are in place to permit users (e.g., federal staff and associates) to update their information through the web interface on the CPA application. The data is available on the phone book.**

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

All users are subject to a Code of Conduct that includes the requirement for confidentiality. **Staff (employees and contractors) received training on privacy and confidentiality policies and practices.** **Access to the PII/BII is restricted to authorized personnel only.** **Access to the PII/BII is being monitored, tracked, or recorded.** **The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.** **The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.** **NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).**
Reason why access to the PII/BII is being monitored, tracked, or recorded:
Access to PII is restricted to only those users who require access and access is monitored and tracked through audit logging functionality.
The information is secured in accordance with FISMA requirements.
Is this a new system? No **Below is the date of the most recent Assessment and Authorization (A&A).** **04/1/2020**
Other administrative and technological controls for the system:

8.2 General description of the technologies used to protect PII/BII on the IT system. *(Includes data encryption in transit and/or at rest, if applicable).*

The system components are administered on internal NIST networks and protected by multiple layers of firewalls and perimeter defenses. Network access controls are employed. The components are located at the NIST Gaithersburg, Maryland facility within the continental United States.

Access logs are kept and reviewed for anomalies on an as needed basis. Transactional audit logging functionality is available to track viewing, modification, and deletion of PII within CPR. **Use of the CPR, Reporting Tool and Attachment Application components are restricted by user authentication, and role-based access is employed across all components. For CPR, the database is encrypted using FIPS 140-2 encryption.** **For the WCM OSAC Membership Application, data collected through the application is encrypted in storage.** **To guard against the interception of communications over the network, the component uses the Transport Layer Security (TLS) protocol which encrypts communications. PII/BII is transferred in a secure fashion using FIPS 140-2 encryption.**

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

Yes, PII/BII is searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

Yes, this system is covered by an existing system of records notice (SORN).
SORN name, number, and link:
NIST-1, NIST Associates **COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies** **COMMERCE/DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs** **COMMERCE/DEPT-25, Access Control and Identity Management System**
SORN submission date to the Department:

Section 10: Retention of Information

10.1 Are these records are covered by an approved records control schedule and monitored for compliance?

Yes, there is an approved record control schedule.
Name of the record control schedule:
GRS 3.1 General Technology Management Records
The stage in which the project is in developing and submitting a records control schedule:
Yes, retention is monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:

10.2 Indicate the disposal method of the PII/BII.

Disposal
Overwriting **Degaussing** **Deleting** **Other (specify)**
Other disposal method of the PII/BII:
The CPR component contains referential data. The CPR marks records as inactive staff for the departed staffs but does not delete them since it is still needed information.

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

11.2 The factors that were used to determine the above PII confidentiality impact levels.

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Identifiability **Obligation to Protect Confidentiality**	**Identifiability - The OSAC Membership Application within the WCM Subsystem stores and processes non-sensitive PII for members of the public applying for OSAC membership.** **Obligation to Protect Confidentiality - Several other systems depend upon CPR.**

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

183-01 interconnects with several other systems. A risk of transmitting PII could exist. However, several security controls are in place to mitigate this risk.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

No, the conduct of this PIA does not result in any required business process changes.
Explanation

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

No, the conduct of this PIA does not result in any required technology changes.
Explanation